UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/614,343	07/08/2003	Gabor Bajko	59643.00228	7843

32294 7590 04/04/2007

SQUIRE, SANDERS & DEMPSEY L.L.P.
14TH FLOOR
8000 TOWERS CRESCENT
TYSONS CORNER, VA 22182

EXAMINER	
FRINK, JOHN MOORE	
ART UNIT	**PAPER NUMBER**
2142	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/614,343	BAJKO, GABOR	
	Examiner	Art Unit	
	John M. Frink	2142	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/29/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

2. Claims 1 – 11, 14 – 17, 19, 20, 22 – 29, 31, 33 – 35, 38, 39 and 43 - 48 are rejected under 35 U.S.C. 102(a) as being anticipated by Jennings and Peterson (RFC 3325 Internet Draft, http://tools.ietf.org/html/draft-ietf-sip-asserted-identity-00, May 27, 2002).

3. Regarding claim 1, Jennings and Peterson show a security server receiving a message; determining whether the message is from a known source or an unknown source and, depending on a result of the determination, modifying the message; and forwarding the message within the telecommunications network (Sections 3 and 5).

4. Regarding claim 2, Jennings and Peterson show receiving a message from outside the telecommunications network (Sections 3, 5 and 10.2).

5. Regarding claim 3, Jennings and Peterson show modifying the message by adding a parameter to the message that indicates that the message has come from a known or an unknown source (Sections 4 and 5).

6. Regarding claim 4, Jennings and Peterson show where the security server is configured to receive a message that includes an identity header and is further

configured to add the parameter to the identity header of the message (Sections 4 and 5).

7. Regarding claim 5, Jennings and Peterson show where the message comprises a SIP message (Section 5).

8. Regarding claim 6, Jennings and Peterson show where the identity header comprises a P-Asserted-Identity (Section 5).

9. Regarding claim 7, Jennings and Peterson show receiving a message that includes an identity header and where said security server is further configured to modify the message by removing at least part of the identity header (Section 7).

10. Regarding claim 8, Jennings and Peterson show a security server configured to detect whether the identity header is of a particular type and if so to remove at least part of the header (Section 7).

11. Regarding claim 9, Jennings and Peterson show where the message comprises a SIP message (Section 7).

12. Regarding claim 10, Jennings and Peterson show detecting whether the identity header comprises a P-Asserted-Identity type (Section 7).

13. Regarding claim 11, Jennings and Peterson show a security server according to claim 1, wherein the security server is configured to determine whether the message is from a known source or an unknown source by determining whether or not the message has been received via a secure means (Sections 9.1 and 11.2 – 11.4).

14. Regarding claim 14, Jennings and Peterson show a network processing element for use in a telecommunications network, the network processing

element configured to: receive a message from another network element; determine whether the message has been modified and, depending on a result of the determination, perform one or more security checks in respect of the message (Sections 4,5, and 11.2 – 11.4).

15. Regarding claim 15, Jennings and Peterson show a network processing element according to claim 14, configured to determine whether an identity header of the message has been modified by detecting whether the identity header of the message includes an added parameter (Section 5).

16. Regarding claim 16, Jennings and Peterson show a network processing element according to claim 15, wherein the message comprises a SIP message (Section 5).

17. Regarding claim 17, Jennings and Peterson show a network processing element according to claim 15, wherein the identity header comprises a P-Asserted-Identity (Section 5).

18. Regarding claim 22, Jennings and Peterson show a telecommunications network comprising a security server and a network processing element, the security server being configured to: receive a message; determine whether the message is from a known source or an unknown source and, depending on a result of the determination, modify the message; and forward the message to the network processing element (Sections 4 and 5).

19. Regarding claim 23, Jennings and Peterson show a telecommunications network according to claim 22, wherein the security server is configured to

receive a message from outside the telecommunications network (Sections 3, 5 and 10.2).

20. Regarding claim 24, Jennings and Peterson show a telecommunications network according to claim 22, wherein the network processing element is configured to: receive a message forwarded by the security server; and determine whether the message has been modified and, depending on the result of the determination, perform one or more security checks in respect of the message (Section 7).

21. Regarding claim 25, Jennings and Peterson show a method of performing a security check on a message in a telecommunications network, the method comprising the steps of: receiving a message; determining whether the message is from a known source or an unknown source and, depending on a result of the determination, modifying the message; and forwarding the message within the telecommunications network. (Sections 3 - 5)

22. Regarding claim 26, Jennings and Peterson show a security server for use in a telecommunications network, the security server configured to: receive a message; determine whether the message is from a known source or an unknown source; and forward the message within the communications network in a manner dependent on a result of the determination (Sections 3 - 5).

23. Regarding claim 27, Jennings and Peterson show a security server according to claim 26, configured to receive the message from outside the telecommunications network (Sections 3, 5 and 10.2).

24. Regarding claim 28, Jennings and Peterson show a security server according to claim 26, configured to forward the message without security, if it is determined that the message is from an unknown source (Section 8).

25. Regarding claim 29, Jennings and Peterson show a security server according to claim 26, configured to forward the message with security, if it is determined that the message is from a known source (Section 8 and 11.2 – 11.5).

26. Regarding claim 31, Jennings and Peterson show a security server according to claim 26, wherein the message comprises a SIP message (Sections 3 -5).

27. Regarding claim 33, Jennings and Peterson show a telecommunications network comprising a security server and a network processing element, the security server being configured to: receive a message; determine whether the message is from a known source or an unknown source; and forward the message to the network processing element in a manner dependent on a result of the determination (Sections 3 - 5).

28. Regarding claim 34, Jennings and Peterson show a telecommunications network according to claim 33, wherein the security server is configured to receive a message from outside the telecommunications network (Sections 3, 5 and 10.2).

29. Regarding claim 35, Jennings and Peterson show the telecommunications network according to claim 33, further comprising: an internal security system, wherein the security server is arranged to forward the message via the internal

security system, if it is determined that a message is from a known source, and wherein the security system is configured to not forward the message via the internal security system, if it is determined that the message is from an unknown source (Sections 8 and 11.2 – 11.5).

30. Regarding claim 38, Jennings and Peterson show a telecommunications network according to claim 33, wherein the message comprises a SIP message (Sections 3 - 5).

31. Regarding claim 39, Jennings and Peterson show a telecommunications network according to claim 33, wherein the security server is configured to determine whether a message is from a known source or an unknown source by determining whether or not the message has been received via a secure means (Sections 9.1 and 11.2 – 11.4).

32. Regarding claim 43, Jennings and Peterson show a method of performing a security check on a message in a telecommunications network, the method comprising the steps of: receiving a message; determining whether the message is from a known source or an unknown source; and forwarding the message within the communications network in a manner dependent on a result of the determination (Sections 3 - 5).

33. Regarding claim 44, Jennings and Peterson show a security server for use in a telecommunications network, the security server configured to: receive a message; and determine whether the message is from a known source or an unknown source and, depending on a result of the determination, determine a subsequent action to be taken in respect of the message (Sections 3 - 5).

34. Regarding claim 45, Jennings and Peterson show a method of performing a security check on a message in a telecommunications network, the method comprising the steps of: receiving a message; and determining whether the message is from a known source or an unknown source and, depending on a result of a determination, determining a subsequent action to be taken in respect of the message (Sections 3 – 5).

35. Regarding claim 46, Jennings and Peterson show a security server for use in a telecommunications network, the security server comprising: receiving means for receiving a message; determining means for determining whether the message is from a known source or an unknown source and, depending on a result of the determination, modify the message; and forwarding means for forwarding the message within the telecommunications network (Sections 3 - 5).

36. Regarding claim 47, Jennings and Peterson show a network processing element for use in a telecommunications network, the network processing element comprising: receiving means for receiving a message from another network element; determining means for determining whether the message has been modified and, depending on a result of the determination, performing one or more security checks in respect of the message (Sections 4, 5 and 11.2 – 11.4).

37. Regarding claim 48, Jennings and Peterson show a security server for use in a telecommunications network, the security server comprising: receiving means for receiving a message; determining means for determining whether the message is from a known source or an unknown source; and forwarding means

for forwarding the message within the communications network in a manner dependent on a result of the determination (Sections 3 - 5).

Claim Rejections - 35 USC § 103

38. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

39. Claims 12, 30, 37 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jennings and Peterson in view of Arkko et al. (US 2002/0052200 A1).

40. Regarding claim 12, Jennings and Peterson show a security server according to claim 11 (Section 3, 5, 11.2).

Jennings and Peterson do not show where the secure means is a Za interface.

Arkko et al. shows where the secure means is a Za interface (Fig. 1, Fig.4, [0040 - 0043]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Jennings and Peterson with that of Arkko et al. in order to utilize a common security protocol which is intended to be used to enable the secure exchange of information in systems like Jennings and Peterson's (Arkko et al., [0040 - 0041]).

41. Regarding claim 30, Jennings and Peterson show a security server according to claim 28 (Section 8).

Jennings and Peterson do not show where the secure means is a Zb interface.

Arkko et al. shows where the secure means is a Zb interface (Fig. 1, Fig.4, [0040 - 0043]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Jennings and Peterson with that of Arkko et al. in order to utilize a common security protocol which is intended to be used to enable the secure exchange of information in systems like Jennings and Peterson's (Arkko et al., [0040 - 0043]).

42. Regarding claim 37, Jennings and Peterson in view of Arkko et al. further disclose a telecommunications network according to claim 35, wherein the internal security system comprises a Zb interface (Peterson, Sections 8 and 11.2 – 11.5; Arkko et al., [0040 - 0043]).

43. Regarding claim 41, Jennings and Peterson in view of Arkko et al. further disclose a telecommunications network according to claim 39, wherein the secure means comprises a Za interface (Peterson, Sections 9.1 and 11.2 – 11.4; Arkko et al., [0040 - 0043]).

44. Claims 13, 21, 32 and 42 rejected under 35 U.S.C. 103(a) as being unpatentable over Jennings and Peterson in view of Soininen (RFC 3574 Internet Draft, http://tools.ietf.org/html/draft-ietf-v6ops-3gpp-cases-00, September, 2002).

45. Regarding claim 13, Jennings and Peterson show a security server according to claim 1 (Section 5).

Jennings and Peterson do not show where the security server comprises an interrogating call session control function.

Soininen shows where the security server comprises an interrogating call session control function (Section 3.2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Jennings and Peterson with that of Soininen in order to provide for an SIP system adhering to the 3GPP networking standard (Soininen, Section 3.2).

46. Regarding claim 21, Jennings and Peterson in view of Soininen further show a network processing element according to claim 14, that comprises a serving call session control function (Jennings and Peterson, Sections 4, 5, and 11.2 – 11.4; Soininen, Section 3.2).

47. Regarding claim 32, Jennings and Peterson in view of Soininen further show a security server according to claim 26, wherein the security server comprises an interrogating call session control function (Jennings and Peterson, Sections 3 – 5; Soininen, Section 3.2).

48. Regarding claim 42, Jennings and Peterson in view of Soininen further show a telecommunications network according to claim 33, wherein the security server comprises an interrogating call session control function (Jennings and Peterson, Sections 3 – 5; Soininen, Section 3.2).

49. Claims 18, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jennings and Peterson in view of Peterson (RFC 3323 Internet Draft, http://tools.ietf.org/html/draft-ietf-sip-privacy-general-00, May 27, 2002).

50. Regarding claim 18, Jennings and Peterson disclose a network processing element according to claim 14 (Sections 4, 5 and 11.2 – 11.4).

Jennings and Peterson do not disclose where said network processing element is configured to determine whether the message has been modified by determining whether all or part an identity header of the message has been removed.

Peterson discloses where said network processing element is configured to determine whether the message has been modified by determining whether all or part an identity header of the message has been removed (Section 6.1).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Jennings and Peterson with that of Peterson so that after header values have been obscured to preserve privacy when communicating with an entity that is not trusted, it is determinable that said header values were originally present so that said header values can said header values may be restored. This enables said header values to be 'recoverable when further messages in the dialog need to be routed to the originating user agent' which is an important part of maintaining header privacy (Peterson, Section 6.1)

51. Regarding claim 19, Jennings and Peterson in view of Peterson further show a network processing element according to claim 18, wherein the message comprises a SIP message (Jennings and Peterson, Sections 4, 5 and 11.2 – 11.4; Peterson, Abstract and Section 6.1).

52. Regarding claim 20, Jennings and Peterson in view of Peterson further show a network processing element according to claim 18, wherein the identity header comprises a P-Asserted-Identity (Jennings and Peterson, Section 5; Peterson, Section 6.1).

53. Claims 36 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jennings and Peterson in view of Haukka (US 2003/0210678 A1).

54. Regarding claim 36, Jennings and Peterson show a telecommunications network according to claim 35 (Sections 8 and 11.2 – 11.5).

Jennings and Peterson do not show where the internal security system comprises a UMTS specified security system.

Haukka shows where the internal security system comprises a UMTS specified security system ([0021 - 0023]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Jennings and Peterson with that of Haukka in order to provide support for a UMTS network, a common environment utilizing SIP (Haukka, Figs. 1 and 2), which is what Jennings and Peterson's disclosure was designed to support (Jennings and Peterson, see title).

55. Regarding claim 40, Jennings and Peterson in view of Haukka further disclose a telecommunications network according to claim 39, wherein the secure means comprises a UMTS standard security means (Jennings and Peterson, Sections 9.1 and 11.2 – 11.4; Haukka, [0021 - 0023]).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John M. Frink whose telephone number is (571)272-9686. The examiner can normally be reached on M-F 7:30AM - 5:00PM EST; off alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571)272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

John Frink

(571) 272-9686

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER